...from concept to acquisition

NAVAL WIRELESS NETWORKS SUMMIT

Sponsored by: NETWARCOM and PEO Ships

Hosted by : SPAWAR AND PEO C4I

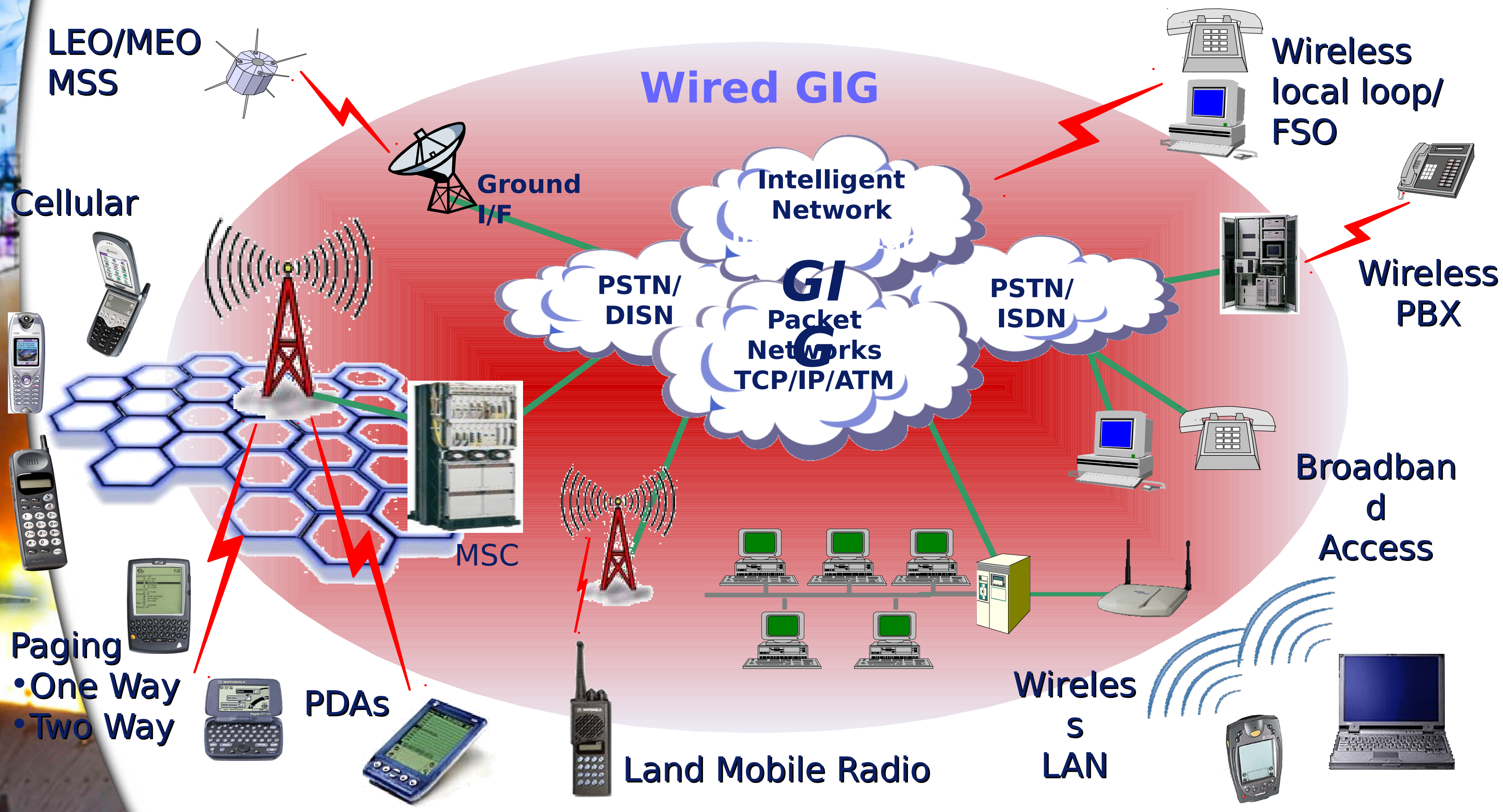
Wireless -- It's here…

Entering
SIMSDALE
FOUNDED 1812
INCORPORATED 1910
WIRED 1955
WIRELESS 2001

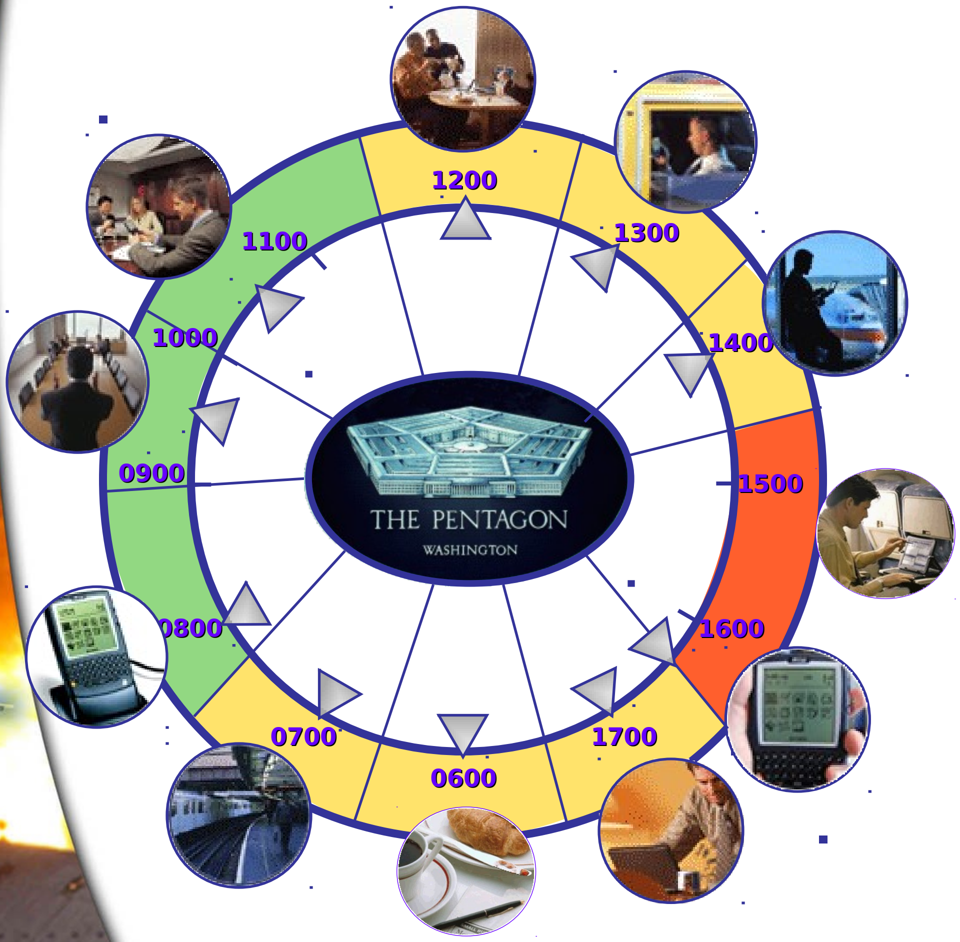
Agenda

- DoD Policy Overview
- Key Policy Mandates
- Supporting and Related Activities
- Knowledge Management
- Opportunities and Challenges

Extending the Global Information Grid (GIG)



A day in the life of a Mobile DoD Worker



0600 – **Checks e-mail from home over breakfast via Blackberry**

0700 – **Files expense report from train via wireless WAN (GPRS/EDGE, EV-DO)**

0800 – **Docks devices at desk and prints report for meeting**

0930 – **Makes live demonstration at a meeting using laptop connected via office WLAN**

1030 – **Sends meeting actions via Blackberry**

1200 – **Collaborates on presentation during lunch via commercial Wi-Fi hotspot**

1300 – **Checks e-mail via Blackberry in taxi to airport**

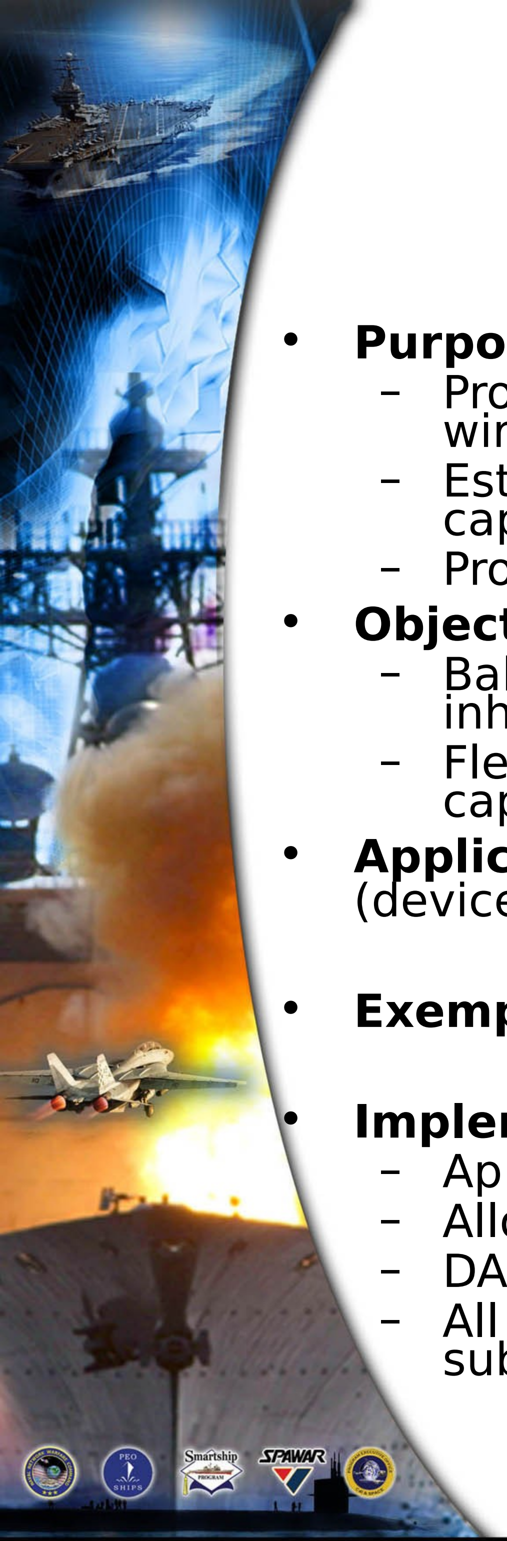
1400 – **Sends updated presentation in airport via public Wi-Fi**

1430-1630 – **Reviews and drafts materials onboard airplane**

1630 – **Checks e-mail via Blackberry coming off the plane**

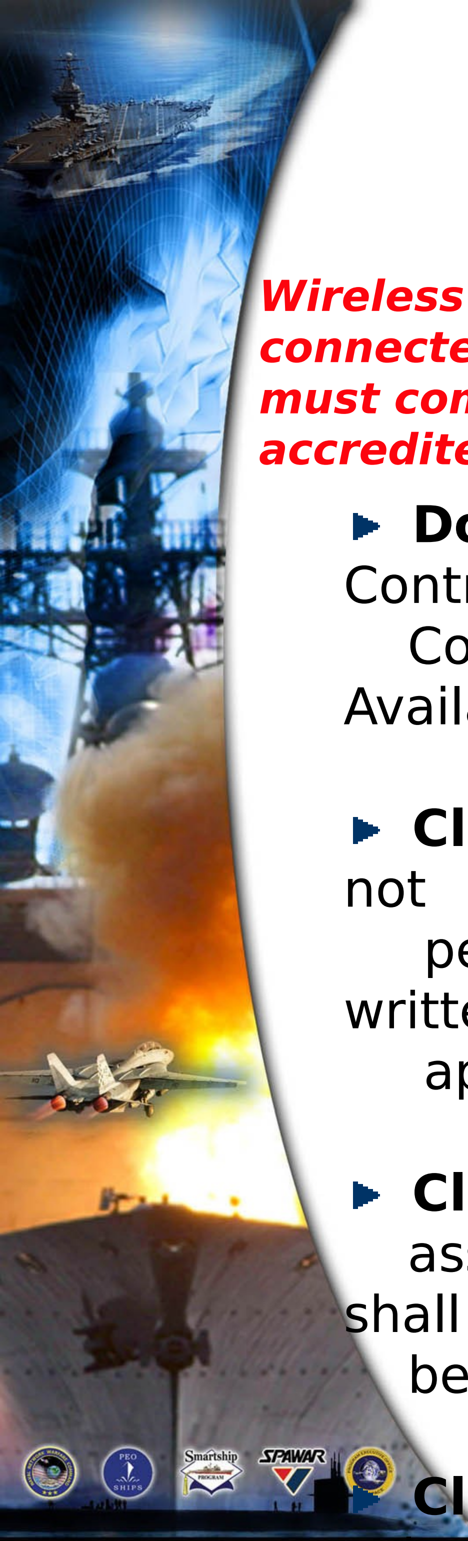
1700 – **Sends report via e-mail connected to hotel broadband Internet connection**

Policy Overview



- **Purpose**:
  - Provides a framework for integrating and leveraging commercial wireless technologies
  - Establish KM process to promote sharing of information on capabilities
  - Promote joint interoperability
- **Objectives**:
  - Balance the tremendous benefits of wireless capabilities with the inherent security risks
  - Flexible enough to allow implementation of Service unique capabilities
- **Applicability**: Commercial wireless devices, services, technologies (devices intended for use in the commercial RF band)
- **Exemptions**: Commercial GPS receivers, medical devices, personal life support etc; also exempted RFIDs from encryption
- **Implementation**:
  - Applies to all new acquisitions
  - Allows for legacy transition
  - DAA has authority to grant case by case exceptions
  - All DoD Components/Activities/Combatant Commanders required to submit plan by November 2004.

DoDD 8100.2 - Security Mandates



Wireless devices, services, and technologies that are integrated or connected to DoD networks are considered part of those networks, and must comply with DoDD 8500.1 and DoDI 8500.2 and be certified and accredited in accordance with DoDI 5200.40…

- **DoDD 8100.2 addresses**: Authentication, Access Control, Confidentiality, Integrity, Non-repudiation, and Availability

- **Classified Areas**: Wireless devices (Cell, RF, IR, etc.) not permitted or operated in classified areas without written approval from the DAA in consultation with CSA CTTA

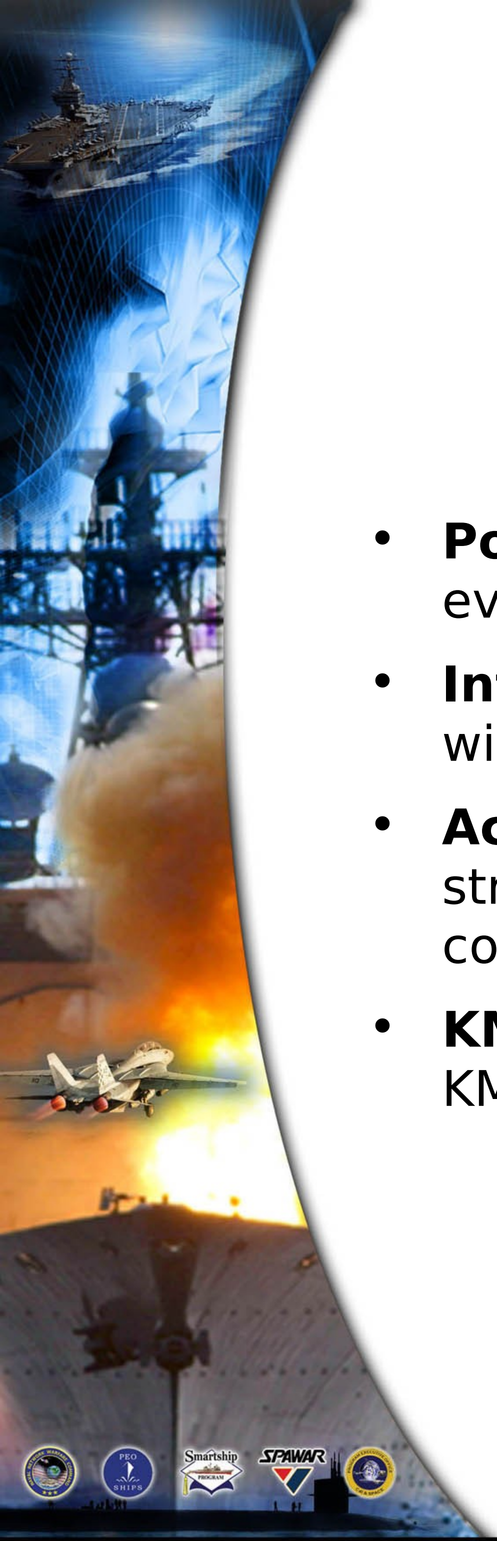
- **Classified Transmission**: If approved by the DAA, only assured channels employing NSA-approved encryption shall be used to transmit classified information

- **Classified Data Storage**: PEDs must be encrypted

DoDD 8100.2 - Additional Mandates

- **Acquisition—**develop acquisition strategies and assess potential architectures (e.g., wireless application frameworks) to minimize costs of wireless development, services and systems, and leverage economies of scale
- **Architecture—**promote the development of wireless application frameworks to extend the GIG to the warfighter and promote interoperability, thus enabling Power to the Edge
- **Joint Operations—**develop, coordinate, and promulgate wireless policies and procedures applicable to Joint operations
- **Interoperability—**ensure appropriate review and identification of key performance parameters and information exchange requirements in capstone and operational requirements documents; implement interoperability testing processes; direct spectrum supportability guidance
- **Knowledge Management—**facilitate collaboration throughout the DoD community on commercial wireless best practices, threats and vulnerability assessment efforts, and vulnerability mitigation solutions.

NII Responsibilities

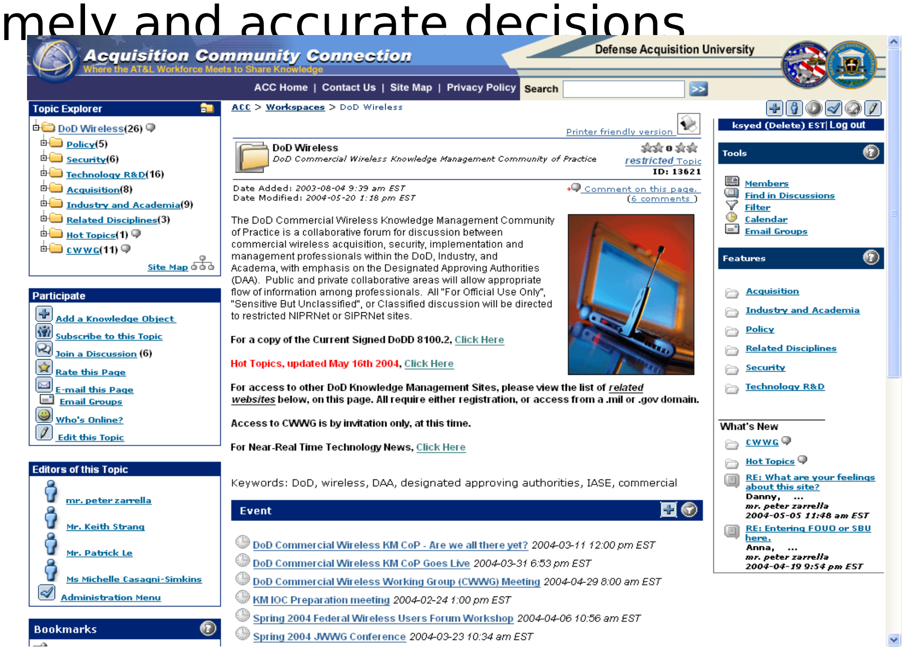


- **Policy**. Oversight of all DoD wireless activities. In addition, evaluate and approve implementation compliance (Nov 04)
- **Interoperability**. Ensure information interoperability of wireless capabilities in support of joint operations
- **Acquisition**. Direct the development of acquisition strategies & assess potential architectures to minimize costs
- **KM/CoP**. Direct the development and implementation of KM process

KM Process

http://acc.dau.mil/wireless

- **Objectives**
  - Maintain sound Department best practices and policies
  - Minimize redundant research endeavors
  - Engage commercial industry through collaboration and exchange o ideas
  - Enable swift and comprehensive implementation guidance
  - Streamline acquisition processes and policy development efforts
  - Enable DAAs to make timely and accurate decisions
- **Topic Areas**
  - Policy
  - Security
  - Acquisition
  - Technology/R&D
  - Industry and Academia
- **Implementation**
  - FOC December 2004



DoD Wireless
DoD Commercial Wireless Knowledge Management Community of Practice

ID: 13621

Date Added: *2003-08-04 9:39 am EST*
Date Modified: *2004-05-20 1:18 pm EST*

The DoD Commercial Wireless Knowledge Management Community of Practice is a collaborative forum for discussion between commercial wireless acquisition, security, implementation and management professionals within the DoD, Industry, and Academa, with emphasis on the Designated Approving Authorities (DAA). Public and private collaborative areas will allow appropriate flow of information among professionals. All "For Official Use Only", "Sensitive But Unclassified", or Classified discussion will be directed to restricted NIPRNet or SIPRNet sites.

For a copy of the Current Signed DoDD 8100.2, Click Here

Hot Topics, updated May 16th 2004, Click Here

For access to other DoD Knowledge Management Sites, please view the list of *related websites* below, on this page. All require either registration, or access from a .mil or .gov domain.

Access to CWWG is by invitation only, at this time.

For Near-Real Time Technology News, Click Here

Keywords: DoD, wireless, DAA, designated approving authorities, IASE, commercial

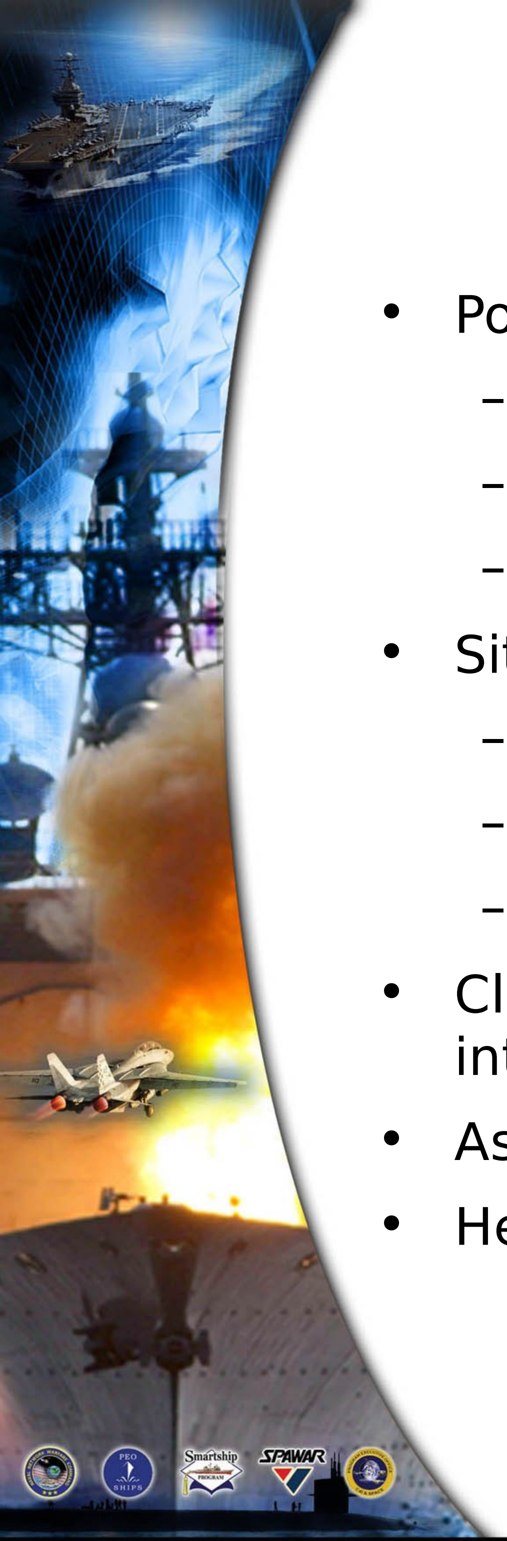
- DoD Commercial Wireless KM CoP - Are we all there yet? *2004-03-11 12:00 pm EST*
- DoD Commercial Wireless KM CoP Goes Live *2004-03-31 6:53 pm EST*
- DoD Commercial Wireless Working Group (CWWG) Meeting *2004-04-29 8:00 am EST*
- KM IOC Preparation meeting *2004-02-24 1:00 pm EST*
- Spring 2004 Federal Wireless Users Forum Workshop *2004-04-06 10:56 am EST*
- Spring 2004 JWWG Conference *2004-03-23 10:34 am EST*

What's New

- CWWG
- Hot Topics
- RE: What are your feelings about this site?
  Danny, ...
  mr. peter zarrella
  2004-05-05 11:48 am EST
- RE: Entering FOUO or SBU here.
  Anna, ...
  mr. peter zarrella
  2004-04-19 9:54 pm EST

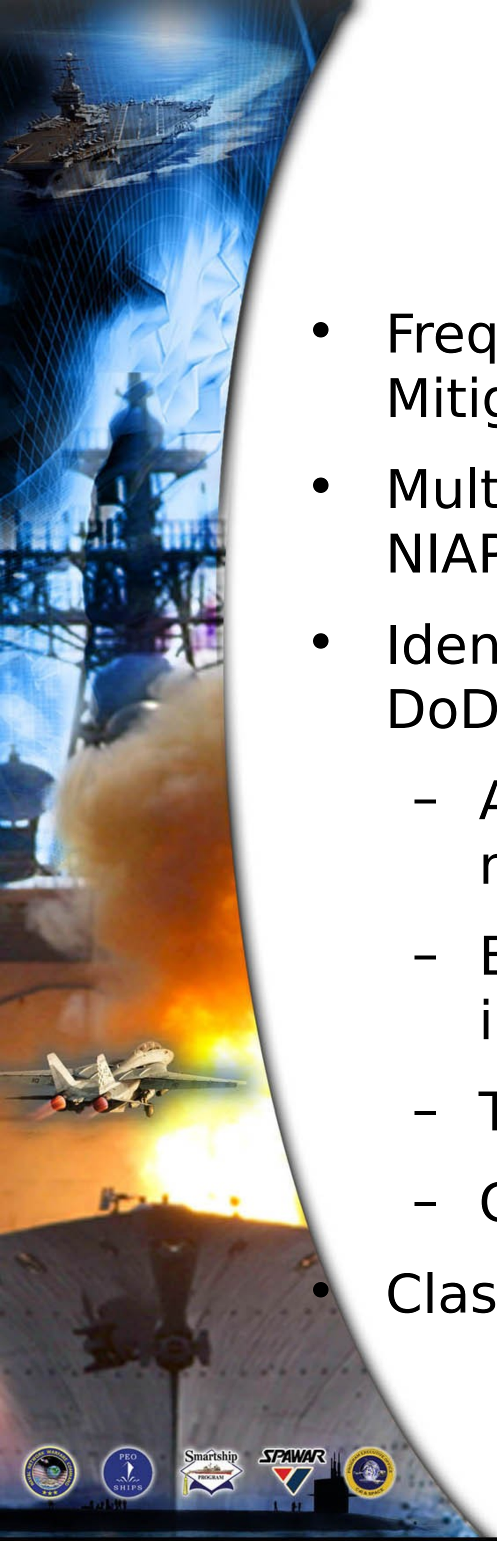
Supporting and Related Activities

Committee on National Security Systems (CNSS) Wireless Working Group (WWG)	Sponsor: ASD(NII)/DCIO Purpose: Provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems
DoD Commercial Wireless Working Group (CWWG)	Sponsor: ASD(NII)/Wireless Directorate Purpose: Discuss, evaluate, and make recommendations regarding DoD commercial wireless activities
Joint Wireless Working Group (JWWG)	Sponsor: NSA Purpose: Identify, characterize, test, and evaluate both COTS and military versions of cellular, personal communications systems (PCS), and wireless local area network (LAN) technologies for joint tactical applications
Pentagon Wireless Technology Working Group (WTWG)	Sponsor: ASD(NII)/DCIO Purpose: Provide planning, configuration management, policies, and procedures for common user wireless technologies and implementations in the Pentagon Area
Federal Wireless Users Forum (FWUF)	Sponsor: NSA and OMNCS Purpose: Identify Federal wireless telecommunication needs and support the interoperability of emerging wireless services and equipment through the formulation of Federal policy, standardization efforts, and other activities



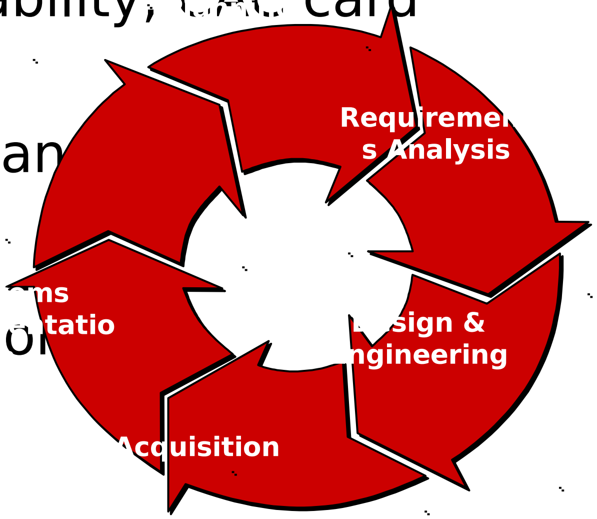
Wireless Opportunities

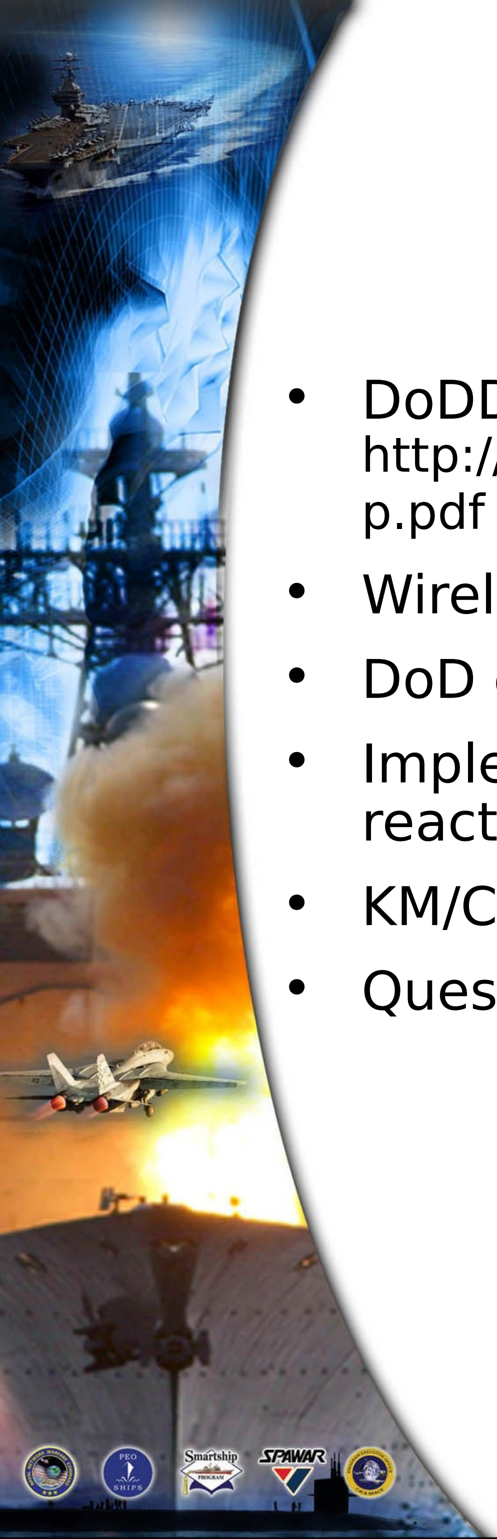
- Post, Camp, and Garrison wireless extensions to the GIG
  - Mobile tactical and business-critical WLANs
  - Limited mobility and fixed WMAN and WWAN broadband
  - Voice over WLAN
- Situational Awareness
  - RFID and Blue Force Tracking
  - Telematics and supply chain sensors
  - Wireless remote sensors and UAVs
- Classified wireless (Classified/Unclassified wireless integration)
- Asset Management
- Health Care



Wireless Challenges

- Frequency Management, Emission Control, and Interference Mitigation
- Multiple C&A processes—NIST Validations, NSA Approvals, NIAP Common Criteria Protection Profiles cross referencing
- Identifying and facilitating industry solutions to adhere to DoD requirements
  - Anti-virus, file encryption, remote security profile management
  - Battery power, size, processing capability, CAC card integration
  - Technology Refresh and Transition Plan
  - Configuration Management
- Classified/Unclassified wireless integration





Summary

- DoDD 8100.2 provides overall commercial wireless policy. http://www.dtic.mil/whs/directives/corres/pdf/d81002_041404/d81002p.pdf
- Wireless offers tremendous opportunities
- DoD elements actively pursuing implementation
- Implementation will be challenging, but developing plan to react to issues
- KM/CoP: http://acc.dau.mil/wireless; FOC December 2004
- Questions:
  - Phone: (703) 602-1734 x 151